Translation for Abstract of Reference 1

The virus library active distribution system, including virus containment node, is characterized by that it possesses a virus centre server and at least a virus subcentre server, and correspondently possesses a tree-like topological three-stage virus containment system formed from virus distribution module of virus centre server, virus distribution module of virus subcentre server and virus library updating module of virus containment node. One virus centre server is positioned at root portion of system, virus subcentre server is positioned in middle layer, all the virus subcentre servers are connected with virus centre server, and the virus containment node is connected with nearest virus subcentre server. The up-to-date virus library is placed on the virus centre server, and the virus distribution module on the virus centre server can automatically transfer most up-to-date virus library. Said invention possesses the advantages of automatically checking and killing up-to-date virus.

[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G06F 12/06

[12]发明专利申请公开说明书

[21]申请号 01139004.2

[43]公开日 2002年5月22日

[11]公开号 CN 1350230A

[22]申请日 2001.12.3 [21]申请号 01139004.2

[71]申请人 复旦大学
地址 200433 上海市邯郸路220号
共同申请人 上海市计算机病毒防范服务中心
[72]发明人 钱松荣 韩苹苹 王 东 余 华
谢 晖 胡方农 周曦民 石 坚
吴恩平 陆金山 杨东升

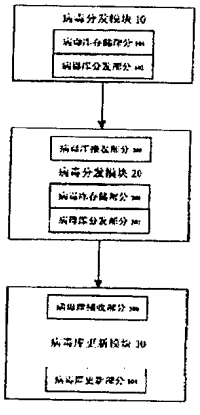
[74]专利代理机构 中原信达知识产权代理有限责任公司
代理人 文 琦

权利要求书3页 说明书8页 附图页数2页

[54]发明名称 病毒库主动分发系统

[57]摘要

一种病毒库主动分发系统，包括病毒防范节点，其特点是设有一台病毒 中心服务器和至少一台病毒分中心服务器，并相应设有病毒中心服务器的病 毒分发模块，病毒分中心服务器的病毒分发模块和病毒防范节点的病毒库更 新模块而构成的树状拓扑三级病毒防范体系。一台病毒中心服务器位于体系 的根部，病毒分中心服务器位于中间层，所有的病毒分中心服务器与病毒中 心服务器相连，病毒防范节点与最近的病毒分中心服务器相连；该病毒中心 服务器上放置最新的病毒库，病毒中心服务器上的病毒分发模块会自动向病 毒分中心服务器发送最新的病毒库；病毒分中心服务器上的病毒分发模块又 会向病毒防范节点发送病毒库，病毒防范节点上的病毒库更新模块完成杀毒 软件中病毒库的自动更新。因此，本发明具有自动查、杀最新病毒的优点。



ISSN1008-4274

权 利 要 求 书

1. 一种病毒库主动分发系统，包括：病毒防范节点（3），其特征在于，设有一台病毒中心服务器（1）和至少一台病毒分中心服务器（2），并相应设有病毒中心服务器（1）的病毒分发模块（10），病毒分中心服务器（2）的病毒分发模块（20）和病毒防范节点（3）的病毒库更新模块（30）而构成的树状拓扑三级病毒防范体系；一台病毒中心服务器（1）位于体系的根部，病毒分中心服务器（2）位于体系中间层，所有的病毒分中心服务器（2）与病毒中心服务器（1）相连，病毒防范节点（3）与最近的病毒分中心服务器（2）相连；该病毒中心服务器（1）上放置最新的病毒库，病毒中心服务器（1）上的病毒分发模块（10）会自动向病毒分中心服务器（2）发送最新的病毒库；病毒分中心服务器（2）上的病毒分发模块（20）又会向病毒防范节点（3）发送病毒库，病毒防范节点（3）上的病毒库更新模块（30）完成杀毒软件中病毒库的自动更新。

2. 根据权利要求 1 所述的病毒库主动分发系统，其特征在于，所说的病毒中心服务器（1）的病毒分发模块（10），其包括病毒库存储部分（101）和病毒库分发部分（102），病毒库存储部分（101）存储病毒中心服务器（1）上最新的病毒定义；该病毒库分发部分（102）取得病毒中心服务器（1）上的最新的病毒库，并以预定的格式发送给各台在病毒中心服务器（1）注册的病毒分中心服务器（2）。

3. 根据权利要求 1 所述的病毒库主动分发系统，其特征在于，所说的病毒分中心服务器（2）的病毒分发模块（20），其包括病毒库接收部分（200）、病毒库存储部分（201）和病毒库分发部分（202）；该病毒库接收部分（200）从该病毒中心服务器（1）的病毒分发模块（10）接收最新的病毒库；该病毒库存储部分（201）在病毒分中心服务器（2）上存储最新的病毒定义；该病毒库分发部分（202）取得病毒分中心服务器（2）上的最新的病毒库，并以预定的格式发送给各台在该病毒分中心服务器（2）注册的病毒防范节点（3）。

4. 根据权利要求 1 所述的病毒库主动分发系统，其特征在于，所说的病毒防范节点（3）的病毒库更新模块（30），其包括病毒库接收部分（300）和病毒库更新部分（301）；该病毒库接收部分（300）从病毒分中心服务器（2）的病毒分发模块（20）接收最新的病毒库；该病毒库更新部分（301）在该病毒防范节点（3）上更新最新的病毒定义，把最新的病毒定义加到病毒特征库中。

5. 根据权利要求 1 所述的病毒库主动分发系统，其特征在于，所说的病毒防范节点（3），包括电子邮件病毒防范服务器、网络文件病毒防范服务器、病毒防范网关和客户端病毒防范软件。

6. 根据权利要求 1 所述的病毒库主动分发系统，其特征在于，所说的病毒分中心服务器（2）系设置于大型企事业单位或区县级病毒防范单位中。

7. 根据权利要求 1 所述的病毒库主动分发系统，其特征在于，所说的病

毒中心服务器（1）系设置于省市级的病毒防范专门机构。

01.12.10

说　　明　　书

病毒库主动分发系统

技术领域

本发明涉及一种计算机病毒库的更新系统，具体地说，是一种病毒库主动分发系统。

背景技术

杀毒软件一般由查杀毒引擎和病毒库组成，杀毒引擎调用病毒库，完成病毒的特征匹配，从而查杀病毒。而病毒库为病毒特征码的集合，各个杀毒软件基本相同。病毒库是杀毒软件中很重要的组成部分，它和杀毒引擎有着不同的特点。杀毒引擎是一成不变的，而病毒库则要时时更新，以保持病毒特征库中的病毒特征码是最新或比较新的，这样才能查杀最新的病毒。所以，病毒库的更新成为杀毒软件的必要的组成部分。现有的杀毒软件中，数据库更新的模式有两种，病毒库补丁方式和在线更新方式。

一、 病毒库补丁方式：用户的杀毒软件中有个独立的病毒特征库，它是软件安装时就有的。为了使用户杀毒软件的病毒库保持最新，计算机安全公司会把最新的病毒特征库放到公司的网站上，用户可以自由下载安装，或是把病毒特征库以售后服务的方式发送给用户，提醒用户更新病毒库。这个病毒库可以是完全的病毒特征库，也可以是病毒特征库的增量，

即新的病毒库可以是完全的覆盖旧的病毒库，也可以是向旧的病毒库中增加新的病毒特征码。这种病毒库补丁方式的优点是用户可以自由选择是否更新病毒库；它的缺点是用户和病毒库服务提供商都要花相当大的工作量以更新病毒库，计算机安全公司必须把最新的病毒库提供给用户，并给用户病毒库升级的说明，而用户被动的接受服务，一旦用户忘记升级病毒库，则杀毒软件就不能防范最新的病毒，如果让用户自己频繁的手动更新病毒库，那是不能忍受的。

二、 在线更新方式：用户的杀毒软件中有个独立的病毒特征库，它是软件安装时就有的，同时杀毒软件中包含了一个在线更新的功能模块，称为 Live Update Virus Definition，病毒库的更新就由这个功能模块完成。用户在打开杀毒软件后，可以选择在线更新病毒特征库，在线更新模块会自动向病毒库的提供者发送更新请求，这要求用户必须是因特网用户，病毒库服务器会响应用户请求，并把最新的病毒特征码发送给用户，用户杀毒软件的在线更新模块把得到的病毒特征码加入病毒特征库，从而完成病毒库的更新。这种病毒库的在线更新方式的优点是极大地减少用户和病毒库服务提供商的工作量；其缺点是用户也是被动的要自己手动更新病毒库，和病毒库补丁方式存在同样的缺点。

发明内容

本发明的目的在于克服现有技术的缺陷，提供一种病毒库主动分发系统，

避免用户手动更新病毒库，实现病毒库的自动更新，减少用户和软件公司的工作量。即用户不用自己手动更新病毒库，病毒库的更新由主动分发模块自动完成。

本发明的技术方案是建立病毒库主动分发系统。它采用三级病毒库分发机制，其包括若干个病毒防范节点，特点是设立一台病毒中心服务器和至少一台病毒分中心服务器，并相应设置该台病毒中心服务器的病毒分发模块，每台病毒分中心服务器的病毒分发模块和每台病毒防范节点的病毒库更新模块，从而形成树状拓扑的三级病毒防范体系：一台病毒中心服务器位于体系的根部，病毒分中心服务器位于体系中间层，所有的病毒分中心服务器与病毒中心服务器相连，病毒防范节点与最近的病毒分中心服务器相连，构成了病毒库的自动更新体系；在病毒中心服务器上放置最新的病毒库，病毒中心服务器的病毒分发模块会自动向病毒分中心服务器发送最新的病毒库，这样，病毒分中心服务器上的病毒库也就是最新的病毒库，病毒分中心服务器的病毒分发模块又会向病毒防范节点发送病毒库，病毒防范节点的病毒库更新模块完成杀毒软件中病毒库的自动更新。

上述病毒中心服务器的病毒分发模块包括病毒库存储部分和病毒库分发部分：该病毒库存储部分存储病毒中心服务器上最新的病毒定义，而病毒库分发部分则取得病毒中心服务器上的最新的病毒库，并以预定的格式发送给各台在中心服务器注册的分中心服务器；

上述的病毒分中心服务器的病毒分发模块包括病毒库接收部分、病毒库存储部分和病毒库分发部分：该病毒库接收部分从病毒中心服务器的病毒分发模块接收最新的病毒库；该病毒库存储部分在病毒分中心服务器上存储最新的病毒定义；该病毒库分发部分取得病毒分中心服务器上的最新的病毒库，并以预定的格式发送给各台在病毒分中心服务器注册的病毒防范节点。

上述的病毒防范节点的病毒库更新模块包括病毒库接收部分和病毒库更新部分：该病毒库接收部分从病毒分中心服务器的病毒分发模块接收最新的病毒库；该病毒库更新部分在病毒防范节点上更新最新的病毒定义，把最新的病毒定义加到病毒特征库中，而可对该防范节点上最新病毒的查杀。

本发明具有显著的效果，它避免了用户手动更新病毒库，实现了病毒库的自动更新，减少了用户和软件公司的工作量，使得杀毒软件自动得到更新，从而能够查杀最新的病毒，避免了新病毒出来时，现有的杀毒软件因没有更新而不能识别的情况。

附图说明

图 1 是本发明的病毒库主动分发模块示意图。

图 2 是本发明的病毒库主动分发系统结构示意图。

具体实施方式

下面根据图 1 和图 2 给出本发明的一个较好的实施例，通过对实施例的描述，进一步给出本发明的技术细节，借以更好地阐明本发明的结构特征和

功能，但它不是用来限制本发明的权利要求保护范围。

请参阅图 1 和图 2，本实施例中包括一台病毒中心服务器 1 和两台病毒分中心服务器 2 以及四台病毒防范节点 3——一台个人计算、一台小型计算机、一台工作站和一台邮件服务器。它们形成树状拓扑三级体系结构，一台病毒中心服务器 1 位于体系的根部，两台病毒分中心服务器 2 位于体系的中间层，它们分别向上连接该病毒中心服务器 1，而向下则分别连接个人计算机与小型计算机；工作站和电子邮件服务器。上述的病毒中心服务器 1 和病毒分中心服务器 2 均安装有系统软件 Linux6.2+Oralce8i+Tomcat。并在病毒中心服务器 1、病毒分中心服务器 2 和病毒防范节点 3 上相应地装上病毒分发模块 10、病毒分发模块 20 和病毒更新模块 30。该三级体系结构中，病毒防范节点 3 包括电子邮件病毒防范服务器、网络文件病毒防范服务器、病毒防范网关和客户端（病毒防范节点 3）病毒防范软件等；病毒分中心服务器 2 适于设在大型企事业单位或区县级病毒防范单位中；而病毒中心服务器 1 则应设在省市级的病毒防范专门机构里。上述的病毒中心服务器 1 的病毒分发模块 10，其包括相连接的病毒库存储部分 101 和病毒库分发部分 102。该病毒库存储部分 101 在病毒中心服务器 1 上存储最新的病毒定义，而该病毒库分发部分 102 则从病毒库存储部分 101 取得最新的病毒库后自动向其下属的病毒分中心服务器 2 发送最新的病毒库；

上述的病毒分中心服务器 2 的病毒分发模块 20，其包括依次连接的病毒

库接收部分 200、病毒库存储部分 201 和病毒库分发部分 202：该病毒库接收部分 200 接收从病毒中心服务器 1 的病毒分发模块 10 发送来的最新的病毒库后，由该病毒库存储部分 201 存储最新的病毒定义，生成病毒分中心服务器 2 上的最新的病毒库，而该病毒库分发部分 202 则取得该最新病毒库后，自动向其下属的病毒防范节点 3 发送该最新的病毒库。

上述的病毒防范节点 3 上的病毒库更新模块 30，其包括病毒库接收部分 300 和病毒库更新部分 301：该病毒库接收部分 300 从病毒分中心服务器 2 的病毒分发模块接收最新的病毒库后，由病毒库更新部分 301 更新最新的病毒定义，把最新的病毒定义加到病毒特征库中。

下面将对病毒防范节点 3 称防范节点、病毒分中心服务器 2（称中级管理中心或称中级）、病毒中心服务器 1（称核心管理中心或称核心）及防范节点—中级、中级—核心间的实现进行详细的描述：

（1） 局域网病毒防范节点 3

局域网病毒防范节点 3 包括多种功能和多种类型，作为病毒防范体系中直接进行病毒查、杀防范的一环，局域网病毒防范节点 3 包括电子邮件病毒防范服务器、网络文件病毒防范服务器、病毒防范网关、客户端（病毒防范节点 3）病毒防范软件等。模型软件中将首先实现客户端（病毒防范节点 3）的病毒防范软件，并着重针对电子邮件型网络化病毒的防范处理。

病毒防范节点 3 从中级病毒管理中心（病毒分中心服务器 2）接收更新的

病毒特征库，获取最新的病毒防范软件版本。

病毒防范节点 3 用接收到的病毒特征库更新本地的病毒特征库。

（2） 中级病毒管理中心（病毒分中心服务器 2）

中级病毒管理中心（病毒分中心服务器 2）维护病毒特征库。

各中级病毒管理中心（病毒分中心服务器 2）服务器将应答客户端（病毒防范节点 3），包括病毒特征库的更新、获取最新的病毒防范软件版本等请求。

各中级病毒管理中心（病毒分中心服务器 2）服务器定时地请求从核心病毒管理中心（病毒中心服务器 1）服务器中获取最新的病毒防范软件版本及相关的病毒特征库。

（3） 核心病毒管理中心（病毒中心服务器 1）

核心病毒管理中心（病毒中心服务器 1）服务器中存放最新的病毒信息库、最新的病毒特征库以及病毒防范软件版本。

核心病毒管理中心（病毒中心服务器 1）自动响应各中级病毒管理中心（病毒分中心服务器 2）服务器对最新的病毒特征库、相关的病毒信息库以及病毒防范软件更新的请求。

（4） 客户端（病毒防范节点 3）—中级

客户端（病毒防范节点 3）与中级病毒管理中心（病毒分中心服务器 2）之间的通信主要为：客户端（病毒防范节点 3）向中级病毒管理中心（病毒分中心服务器 2）请求病毒特征库/病毒防范软件的更新和中级病毒管理中心

（病毒分中心服务器 2）对客户端（病毒防范节点 3）请求的响应；以及客户端（病毒防范节点 3）向中级病毒管理中心（病毒分中心服务器 2）提交病毒信息的请求及中级病毒管理中心（病毒分中心服务器 2）的确认。

（5）中级一核心

中级病毒管理中心（病毒分中心服务器 2）与核心病毒管理中心（病毒中心服务器 1）之间的通信主要为：中级病毒管理中心（病毒分中心服务器 2）向核心病毒管理中心（病毒中心服务器 1）请求病毒特征库更新和核心病毒管理中心（病毒中心服务器 1）对中级病毒管理中心（病毒分中心服务器 2）请求的响应；以及中级病毒管理中心（病毒分中心服务器 2）向核心病毒管理中心（病毒中心服务器 1）提交病毒信息的请求及核心的确认。

说明书附图

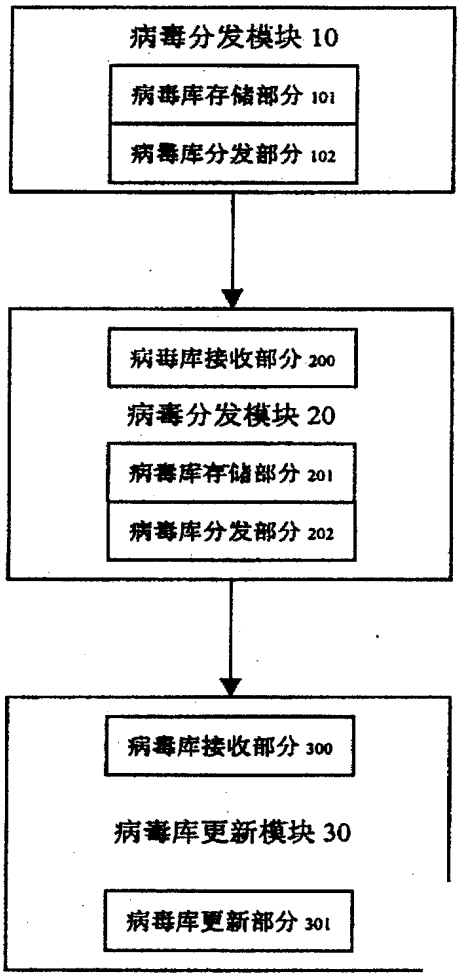

病毒分发模块 10
病毒库存储部分 101
病毒库分发部分 102
病毒库接收部分 200
病毒分发模块 20
病毒库存储部分 201
病毒库分发部分 202
病毒库接收部分 300
病毒库更新模块 30
病毒库更新部分 301

图 1

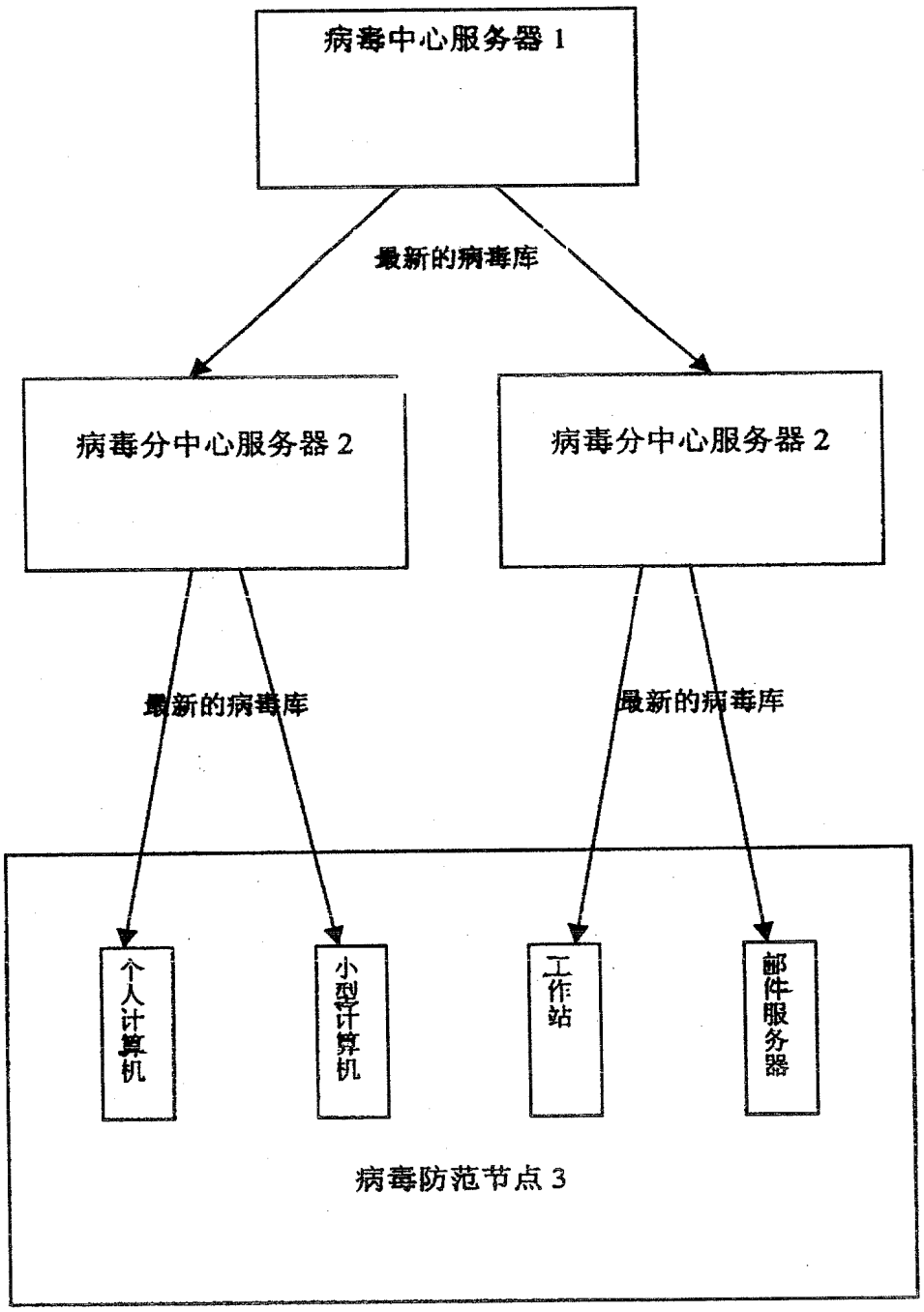

病毒中心服务器 1
最新的病毒库
病毒分中心服务器 2
病毒分中心服务器 2
最新的病毒库
最新的病毒库
个人计算机
小型计算机
工作站
邮件服务器
病毒防范节点 3

图 2